2025 Trend Report

FOR THE CYBERSECURITY LANDSCAPE

HUNT & HACKETT

"It feels like we're fighting cybercrime with one hand tied behind our backs."

Jurjen Harskamp,
Co-founder & CEO at Hunt & Hackett

Table of Contents

Executive Summary 2

Chapter 1: The Democratization of Cybercrime 4

1.1 Key trends 4
1.2 Low costs, high rewards, and anonymity fuel growth 5
1.3 Locked out: Power shifts in the RaaS ecosystem 6
1.4 You've got mail: The rise of Business Email Compromise 8
1.5 Initial Access Brokers shift to edge devices 10
1.6 CaaS in Numbers 11
1.7 The Hunt & Hackett perspective 12

Chapter 2: The Impact of Artificial Intelligence 13

2.1 Key trends 13
2.2 AI advances cybercrime tactics, but falls short of true innovation 14
2.3 Defensive potential (and pitfalls) 15
2.4 The Hunt & Hackett perspective 17

Chapter 3: The Influence of Nation States 18

3.1 Key trends 18
3.2 Lines blur between APTs and cybercriminals 18
3.3 Nation-state activity focused on conflict zones 19
3.4 Critical infrastructure under siege 21
3.5 The Hunt & Hackett perspective 22

Chapter 4: The NIS2 Directive 23

4.1 Key trends 23
4.2 Cybersecurity will become a boardroom issue 24
4.3 Companies face increased reporting obligations 24
4.4 Barriers to information sharing 26
4.5 Oversight of digital supply chains 26
4.6 Not just a box-ticking exercise 27
4.7 The Hunt & Hackett perspective 29

References 30

Executive Summary

The cyber threat landscape is becoming increasingly complex, marked by a surge in sophisticated attacks and heightened activity from Advanced Persistent Threats (APTs). At the same time, technological advancements like AI are reshaping offensive tactics, creating new challenges for governments and businesses alike. This report brings together insights from both public and private sector experts, with the goal of helping Dutch organisations understand the shifting dynamics of cybersecurity in 2025. Our aim is to provide practical guidance for building resilience in the face of these emerging threats, while offering our own (admittedly subjective) perspectives on what lies ahead.

The cybersecurity landscape in 2025 is shaped by four critical trends:

- **Cybercrime is becoming more accessible**, thanks to the rise of Cybercrime-as-a-Service platforms that offer ready-made tools and services for launching attacks. At the same time, many cybercriminals operate freely from countries that offer them protection or turn a blind eye to their activities, further contributing to the growth of this ecosystem.

- **Artificial Intelligence is enhancing both offensive and defensive capabilities**. Attackers are leveraging Gen-AI to support social engineering and reconnaissance efforts, while defenders are still navigating the hype, with practical applications yielding incremental advances rather than transformative breakthroughs.

- **Nation-state actors are increasingly sophisticated**, embedding cyber operations into broader hybrid warfare strategies that target critical infrastructure and blur the lines between state and criminal activities.

- Meanwhile, **increasing regulation, particularly the NIS2 Directive, is pushing cybersecurity into the boardroom**, raising important questions about how compliance frameworks can be implemented without stifling innovation or turning security into a box-ticking exercise.

These trends reflect a cybersecurity landscape that is more complex, interconnected, and challenging than ever before. Building a safer, more resilient society requires a nuanced understanding of these dynamics. Knowledge and awareness are the first steps to fostering meaningful change, and this report is designed to empower organisations with the insights needed to adapt and thrive in this evolving environment.

Thank you to our contributors

Ernst Noorman
Ambassador-at-Large for Cyber Affairs

Kelvin Rorive
CISO at ICT Group

Gijs Roeffen
CISO at Castor

Moshgan Wahedi
NIS2 and Netcode Program Manager at NCSC-NL

Fleur van Leusden
Cybersecurity adviser & creator of the CISO Praat podcast

Anton Chuvakin
Senior security staff, Office of the CISO, Google Cloud

Jurjen Harskamp
Co-founder and CEO at Hunt & Hackett

Ronald Prins
Co-founder at Hunt & Hackett

Rebecca Lumley
Strategic Threat Intelligence Analyst at Hunt & Hackett

CHAPTER ONE

The Democratization of Cybercrime

Cybercrime is no longer the exclusive domain of highly skilled hackers. Over the past few years, the landscape has undergone a fundamental shift with the rise of Cybercrime-as-a-Service (CaaS). Much like its legitimate counterpart, Software-as-a-Service (SaaS), the CaaS model packages tools, techniques, and infrastructure into easy-to-use services available for purchase.

Today, anyone with a motive - and a (surprisingly) modest budget - can wield the power of offensive cyber tools that once required advanced technical expertise to develop. Looking ahead to 2025 and beyond, this ecosystem shows no signs of slowing down. Advances in AI are likely to make CaaS offerings more sophisticated and scalable, amplifying the risks they pose to businesses and governments alike.

Key trends

- Increasing availability of CaaS tools and services, combined with the anonymity enabled by cryptocurrencies, creates powerful economic incentives to engage in cybercrime.
- Law enforcement actions have contributed to a shift in the Ransomware-as-a-Service (RaaS) landscape, creating new opportunities for groups like RansomHub and Akira.
- Business Email Compromise now surpasses ransomware in financial impact, driven by its (relative) simplicity, low risk, and high success rate. Simultaneously, BEC attacks are becoming more technically sophisticated.[1]
- Initial Access Brokers are expanding their clientele to include APTs while also shifting their targeting from Remote Desktop Protocol (RDP) to VPNs, mirroring the broader trend of cybercriminals focusing on network edge technology.

Low costs, high rewards, and anonymity fuel growth

The CaaS ecosystem thrives on accessibility, anonymity, and powerful economic incentives, making cybercrime an increasingly attractive venture. Today, the tools required to execute a successful cyberattack are often just a click away, readily accessible on dark web marketplaces and messaging platforms such as Telegram. Many CaaS operators host clean, professional online storefronts and even offer customer service and loyalty programs, mirroring legitimate e-commerce platforms.

Cryptocurrencies enable anonymous transactions, while CaaS intermediaries obscure the true source of attacks. For example, an operation leveraging LockBit 3.0 ransomware might be traced back to the LockBit group, but identifying the specific affiliate who purchased and deployed the malware is far more challenging.

Compounding this issue is the political safeguarding cybercriminals receive in certain regions. In nations where cybercrime against Western targets is ignored - or even tacitly encouraged - threat actors operate with little fear of prosecution.

"It feels like we're fighting cybercrime with one hand tied behind our backs. The reality is that certain countries have little incentive or intention to prevent attacks against Western organisations. If the Big Four (Russia, China, Iran, North Korea) were removed from the equation, cybercrime would be significantly reduced. Unfortunately, international cross border cooperation with these countries is pretty much off the table."

Jurjen Harskamp
Co-founder and CEO at Hunt & Hackett

Together, these factors create a highly favorable risk-reward ratio for cybercriminals. The costs of launching a cyberattack, whether through ransomware, BEC, or other means, are typically negligible compared to the potential financial gain. Experts argue that to make a meaningful impact on cybercrime, the underlying incentive structures must change.

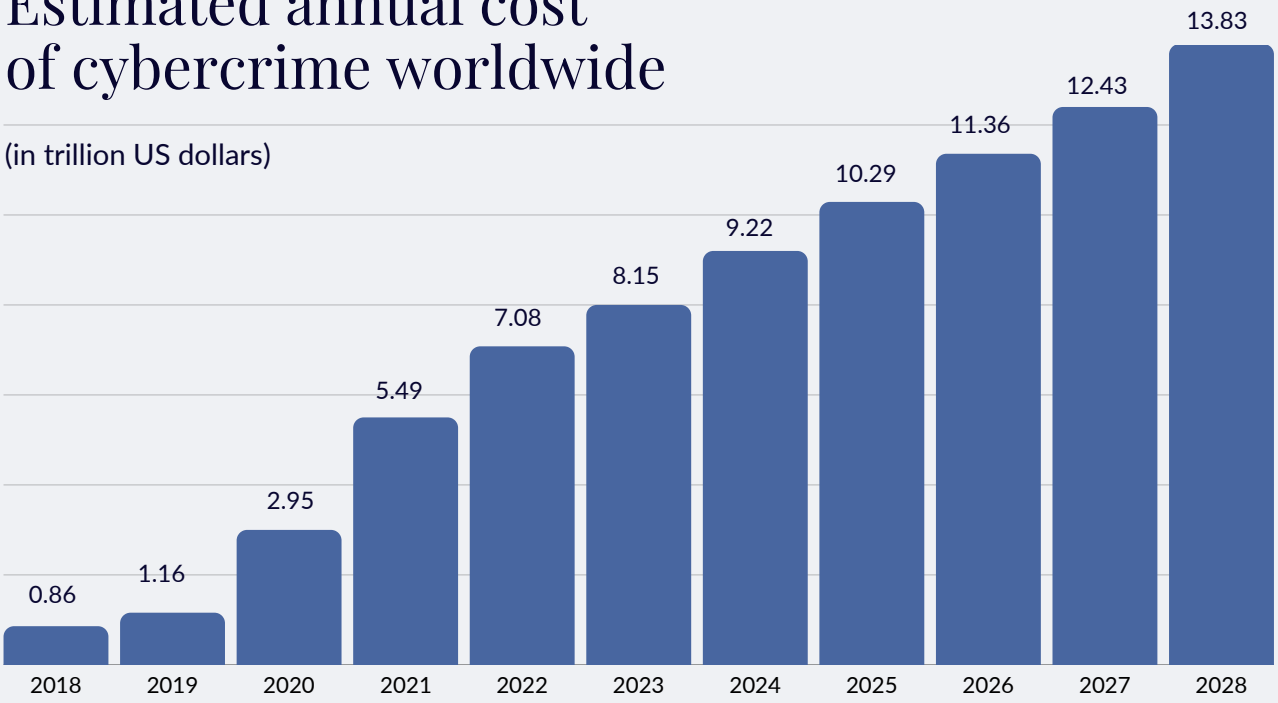
"We need to find ways to make hacking expensive. In my previous experience in the financial sector, the focus wasn't on directly targeting the criminals, but rather on dismantling the money mills. Without a way to cash out their stolen funds, criminals lose their incentive to attack."

Kelvin Rorive
CISO at ICT Group

Looking at 2025, the CaaS ecosystem will likely continue to grow in scale and sophistication. With limited hope for international cooperation, novel solutions will be required to undermine the incentive structures fueling CaaS - making it riskier, costlier, and ultimately less attractive to engage in cybercrime.

Estimated annual cost of cybercrime worldwide

(in trillion US dollars)



Source: Statista

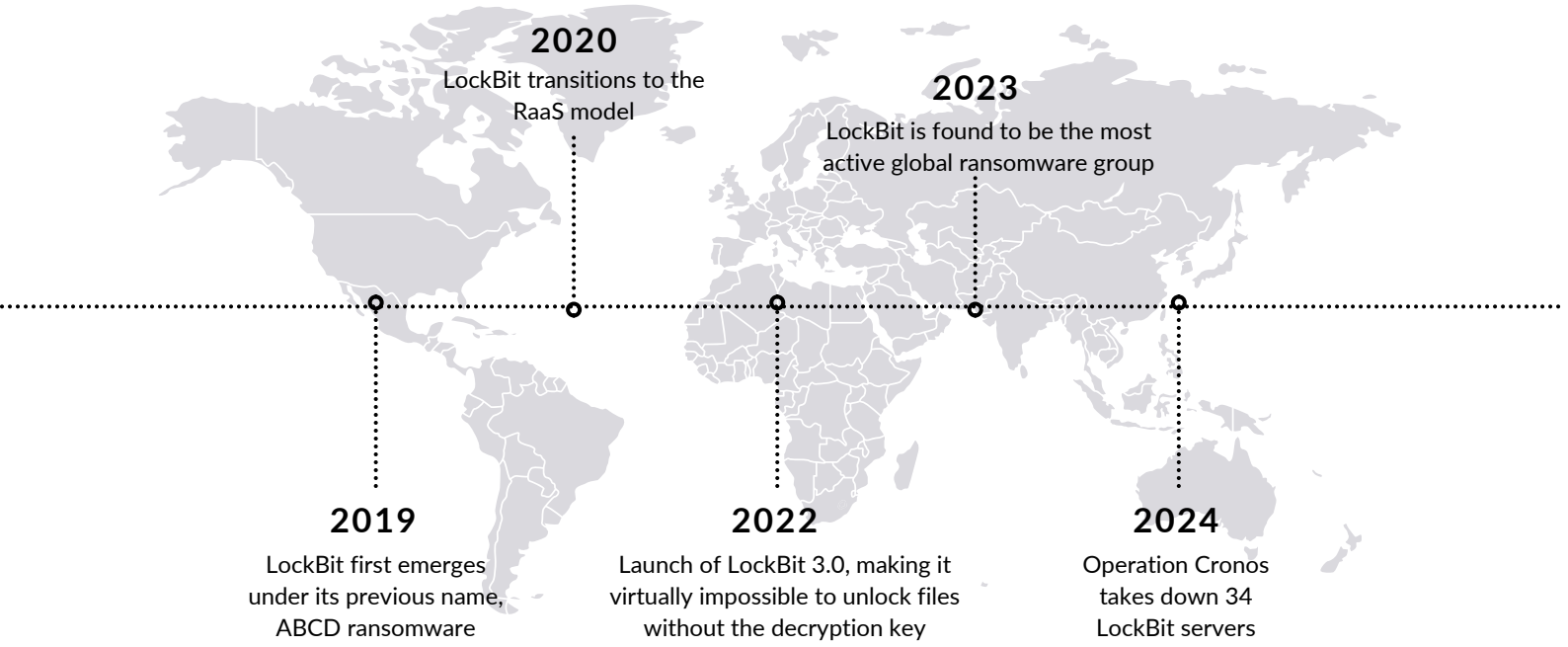
Locked out: Power shifts in the RaaS ecosystem

Ransomware-as-a-Service (RaaS) continues to dominate the cybercrime ecosystem, with ransomware claims reaching an all-time high in November 2024.[2] However, the RaaS landscape looks markedly different than it did just one year ago.

In February 2024, international law enforcement launched Operation Cronos, a joint operation that seized control of LockBit's primary platform and other critical infrastructure. This was a highly significant blow, as LockBit had been the most active global ransomware group and RaaS provider in 2022 and 2023.[3]

Less than two weeks later, BlackCat - the second most prolific ransomware gang of 2023 - shut down its dark web site and uploaded a law enforcement seizure banner, which many believe was actually an exit scam.[4] While LockBit attempted to rebuild, its activity remained low throughout mid-2024. Evidence suggests the group resorted to re-posting old victims on its leak site to inflate its numbers and project an image of normal operations.[5]

In May 2024, the U.S. Department of Justice charged the group's suspected leader, Russian national Dimitry Khoroshev (known as LockBitSupp), offering a reward of up to $10 million for information leading to his arrest and conviction. By June 2024, the FBI announced it had acquired 7,000 LockBit decryption keys, urging victims to come forward.[6]



These events created a power vacuum, allowing new players to rise to prominence. Of these, RansomHub appears to be leading the charge, having claimed 500 victim organisations in the second half of 2024 alone. According to ESET, the group is likely to remain the most active in 2025, followed by groups such as Akira, Kill Security, SAFEPAY, and Qilin. Researchers believe RansomHub is likely made up of former LockBit and BlackCat members.[7]

This rapid turnover underscores the cyclical nature of the ransomware ecosystem. Disruptions may force groups to rebrand or reorganize, but they do little to alter the underlying dynamics. Recent law enforcement action demonstrates that this threat is being taken seriously, but international cooperation is required to truly bring ransomware operators and affiliates to account. In the meantime, experts highlight the importance of tackling RaaS from a variety of angles.

"What I'm seeing is that law enforcement is quite creative in targeting these [ransomware] groups. They're not just going after the individuals, they're also going after the ISPs, cloud service providers, and the domain name registrars – the companies that facilitate these criminals. And that's very useful because if you cannot get a platform, well, good luck with your ransomware group. Will it eradicate this behavior completely? No – it'll always be a cat and mouse game. But we are seeing that it has some effect."

Fleur van Leusden
Cybersecurity adviser & creator of the CISO Praat podcast

You've got mail: The rise of Business Email Compromise

Business Email Compromise (BEC) has quietly overtaken ransomware as the most financially damaging form of cybercrime, with adjusted annual losses totaling $2.9 billion in 2023, compared to just $59.6 million for ransomware.[8] Despite their impact, BEC attacks are far more low-level and discreet – they rarely produce external signals and companies have little incentive to announce they've been compromised.

"Ransomware is all over the news because people notice if a company's network goes down, it's hard to keep it a secret. But if a company loses €100,000 to Business Email Compromise, they're not going to disclose it."

Ronald Prins
Co-founder at Hunt & Hackett

The prevalence of BEC has been rising steadily over the past few years, driven by its (relative) simplicity and low risk. Unlike ransomware - which requires significant technical expertise and infrastructure - BEC scams rely on social engineering and exploiting trust in email communications. These attacks are quick, low-cost, and (potentially) quite lucrative, making them attractive to financially motivated cybercriminals.

"Business Email Compromise is easy to execute, it's even fun to some extent. If you look at it from the cybercrime perspective, the chances of getting caught are very low, and it has a high success rate."

Gijs Roeffen
CISO at Castor

Introducing BEC 2.0

At Hunt & Hackett, we've observed BEC incidents growing more sophisticated, moving beyond traditional social engineering techniques and increasingly incorporating an adversary-in-the-middle (AiTM) component to bypass multi-factor authentication (MFA). This shift is likely a response to the widespread adoption of MFA, which has made simple credential phishing less effective.

How does AiTM work?

Adversary-in-the-middle (AiTM) attacks deceive users into entering their credentials and MFA codes on a phishing website controlled by the attacker, who then relays the data to the legitimate email provider in real time. This enables the attacker to steal the session token, granting them access to the victim's account without needing the credentials again until the token expires - typically 90 days by default for Microsoft accounts. [9]

The execution of such attacks is straightforward; open-source tools facilitate most of the setup, leaving attackers with little more to do than register a domain for the phishing site. Although these attacks are becoming more advanced, they don't necessarily require more effort - suggesting that BEC will remain a problem for businesses for quite some time to come.

Detecting and mitigating multi-stage BEC and AiTM attacks

The good news is that BEC attacks are detectable if the appropriate measures, such as Managed Detection and Response (MDR), are in place. Anomalous behaviours, such as impossible travel, token reuse across multiple devices, or unusual session persistence, serve as potential indicators of such an attack.

There are also reliable solutions that can prevent BEC and AiTM attacks outright. Microsoft recommends Passkeys, which use public-private key cryptography, as a gold-standard defence. Similarly, hardware authentication devices like YubiKeys offer strong protection, despite the logistical challenges of deploying them across an enterprise at scale. Organisations that choose not to implement these solutions are knowingly accepting the risk, leaving themselves vulnerable to attacks that are otherwise preventable.

Initial Access Brokers shift to edge devices

Initial Access Brokers (IABs) play a pivotal role in the Cybercrime-as-a-Service ecosystem by selling access to compromised corporate networks. These actors have been evolving in recent years, both in terms of their clientele and attack methods. Once primarily catering to cybercriminal groups, IABs are now increasingly supplying state-sponsored APTs as well, further blurring the lines between financially motivated cybercrime and nation-state operations. This overlap is explored in the following section, The Influence of Nation-States.

At the same time, IABs have shifted their tactics. While they previously focused on exploiting Remote Desktop Protocol (RDP) servers to gain initial access to corporate networks, VPN access surpassed RDP as the primary entry point in 2024. This aligns with a broader trend of cybercriminals increasingly targeting network edge devices.[11]

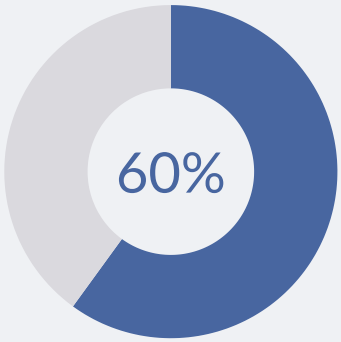
Edge devices - such as firewalls, routers, email gateways, and VPN gateways - are difficult to monitor, making them especially vulnerable to cyberattacks.

By default, these devices are often excluded from regular Managed Detection and Response (MDR) services, with only a few providers accepting data from them.

This is largely due to the high cost of device-specific configurations, variations in log details and the ability to forward logs, and the economics of data ingestion for MDR providers. [12]

This has made edge devices attractive targets for hackers, and critical vulnerabilities have been widely exploited in technologies like Cisco XE, Citrix Bleed, FortiGuard FortiOS, and MOVEit secure file transfer software.

A recent WithSecure analysis found that CVEs discovered in edge devices doubled between 2022 and 2023 and continued to climb in 2024.



Even more concerningly, zero-day exploits accounted for 60% of vulnerabilities identified in network edge technology.[13]

This evolution underscores the adaptability of IABs and exposes a persistent gap in corporate defences. To address these blind spots, organisations should proactively patch vulnerabilities as they emerge, as well as ensuring that edge devices are monitored for anomalous activity.

Committing cybercrime: What does it cost for actors?

$5 +

A 300-second **DDoS attack** using a 125 Gbps botnet can cost as little as $5, while a 10,800-second attack may cost $60 (approximately $20 per hour). Prices depend on the target's protection measures, such as traffic filtering, and the botnet's operational costs. [16]

$20 +

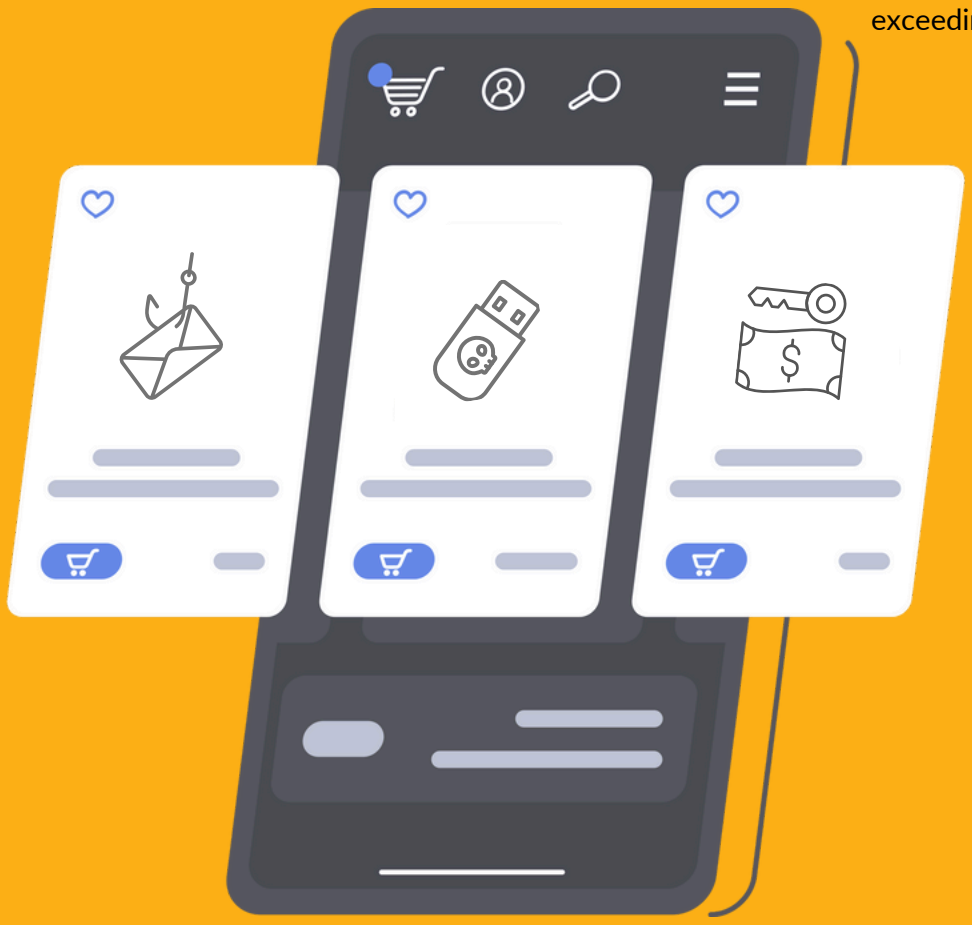
Phishing kits are generally priced between $20 and $880, with an average cost of around $300. [15]

$40 +

Ransomware-as-a-Service (RaaS) kits typically range from $40 per month to several thousand dollars. [14]

$500 +

Access to corporate networks through **Initial Access Brokers** typically costs $500 to $2,000, with high-value listings occasionally exceeding $10,000. [17]



The Hunt & Hackett perspective

2024 proved that disrupting cybercrime is not the same as dismantling it. While initiatives like Operation Cronos demonstrate that coordinated law enforcement efforts can shake up the ransomware landscape, they unfortunately do little to alter the underlying dynamics. Groups dissolve, rebrand, and resurface, often with the same members operating under a different name. As long as major cybercrime hubs - Russia, China, Iran, and North Korea - continue to provide safe haven for these actors, the cat-and-mouse game looks set to continue.

Meanwhile, the evolving tactics of BEC attackers and Initial Access Brokers send a clear message: cybercriminals are more than capable of adapting to defensive measures, meaning blue teamers must move quickly to stay one step ahead.

CHAPTER TWO

The Impact of Artificial Intelligence

The proliferation of Artificial Intelligence (AI) in cybersecurity presents a complex duality. On one hand, attackers are leveraging AI to automate and enhance their campaigns, posing new challenges for defenders. On the other hand, the defensive potential of AI - while promising - is still limited and may, at times, be overvalued.

As we move into 2025, the challenge will be striking a balance: leveraging AI effectively on the defensive side while maintaining a critical perspective and staying ahead of adversaries who are increasingly exploiting its capabilities. This section will explore the benefits and challenges of AI on both sides of the digital battlefield.

Key trends

- Attackers are effectively leveraging AI to enhance reconnaissance and social engineering, enabling highly targeted and convincing campaigns that exploit trust and vulnerabilities with increasing precision. Despite these advances, more novel or damaging use cases have yet to be seen.
- AI offers numerous practical applications for defenders, including intelligence gathering, anomaly detection, asset management, and reporting. However, defenders should prioritize incremental improvements rather than relying on AI to solve cybersecurity's most complex challenges.

AI advances cybercrime tactics, but falls short of true innovation

Two key areas where AI has meaningfully enhanced attackers' capabilities are reconnaissance and social engineering. In the preparation phase of an attack, generative AI tools can be used to support target selection and background research, as well as with the identification of weak points in a company's defenses. This is achieved by harvesting contextual data from sources like social media, public statements, and leaked documents.

One striking example comes from Castor, where Gijs Roeffen, CISO, described the results of AI-enabled phishing simulations. By leveraging public information from LinkedIn, the AI tool identified the timing of a company party - a period when employees were consuming alcohol and likely less alert. It then launched a targeted phishing attack during this window, achieving an 80% success rate compared to the usual 12-15% seen in non-AI-enabled tests.

Additionally, the proliferation of Large Language Models (LLMs) such as ChatGPT has significantly enhanced the ability of attackers to conduct effective social engineering attacks. Ronald Prins, co-founder at Hunt & Hackett, notes, "It's very easy to set up a perfect email now without speaking the language," while Gijs Roeffen recalls observing "completely spotless" social engineering campaigns that successfully mimicked the company's tone of voice and usual communication style.

"It was insanely scary and impressive."

Gijs Roeffen
CISO at Castor

By generating flawless, personalised messages, AI enables attackers to exploit trust and manipulate targets with unprecedented precision. Looking ahead, the widespread availability of LLMs and the integration of AI into CaaS tools will continue to increase attackers' capabilities in reconnaissance and social engineering.

However, we have yet to see evidence of more novel or groundbreaking applications of AI on the offensive side, as the technology's potential remains largely focused on refining existing tactics. One major impediment for attackers relates to the availability of training data - a resource that is often scarce or difficult to obtain in the context of malicious activities. As a result, while AI can assist attackers in automating and scaling certain tasks, its ability to drive groundbreaking offensive techniques remains limited - at least for now.

"If you want to use AI to its full potential, you need a lot of data. Hacker data, however, makes up only a tiny fraction of what's available online, it's very limited. So, I don't foresee a situation where the use of AI is really transformative for attackers. Of course, for more low-level use cases like social engineering, it's very useful. But will AI drive groundbreaking innovations on the offensive side? Personally, I don't think so."

Ronald Prins
Co-founder at Hunt & Hackett

However, while AI has yet to demonstrate transformative offensive capabilities, it would be premature to dismiss its future potential.

"We may not see AI acting as an autonomous offensive agent anytime soon, but it's already proving useful in the background - automating reconnaissance, adapting malware to create new variants with the aim to bypass detection, and identifying vulnerabilities more efficiently. Today, its impact remains incremental, but if attackers get their hands on large pentest datasets or integrate AI into expansive botnets, for example, we could see a fundamental shift in offensive AI capabilities."

Jurjen Harskamp
CEO at Hunt & Hackett

Defensive potential (and pitfalls)

On the defensive side, the integration of AI isn't exactly new - it has long been embedded in cybersecurity tools such as antivirus software and network detection and response (NDR) solutions. However, these earlier applications primarily relied on machine learning for statistical anomaly detection and pattern recognition, rather than the generative AI capabilities we see today. While LLMs introduce new possibilities, increased attention on AI may have contributed to an influx of inflated claims and underwhelming solutions entering the market.

"I'm not one of those people that believes that AI is going to fundamentally change cybersecurity, and I'm kind of wary of all these snake oil salesmen jumping on the bandwagon, shouting: 'Our product has AI'. That's lovely, but AI has been a part of antivirus software, as an example, for years. Sure, it's the next big thing - but it's not revolutionary."

Fleur van Leusden
Creator of the CISO Praat podcast

Despite this, there are many highly practical examples of how AI is being leveraged by cybersecurity professionals. For instance, Kelvin Rorive, CISO at ICT Group, describes using an AI tool to identify his company's exposed assets on the internet and determine which systems are most vulnerable. His organisation also recently implemented an AI-powered chatbot to provide employees with instant answers to security questions and guidance on company policies.

"Personally, I'm always looking for innovative solutions and I tend to give more trust to the innovation rather than focusing on the limitations. It's a bit of an odd thing to say as a CISO, but I think that if you give space for innovative solutions, it will benefit you in the end and ultimately make things more secure. But of course, you should always remain critical and question yourself about the purpose of having AI as part of a specific application."

Kelvin Rorive
CISO at ICT Group

Beyond these practical examples, large-scale adoption of AI among defenders is still lagging. Many organisations are hesitant due to the current limitations, such as hallucinations, a high rate of false positives, lack of insight into decision-making and its inability to adapt to nuanced security environments.

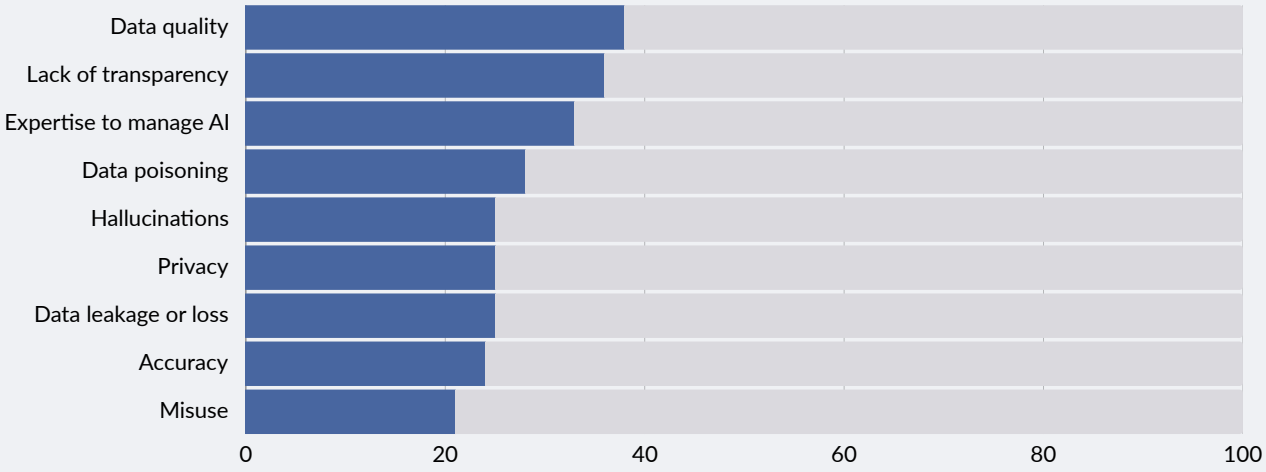
"AI still makes a lot of errors, but it can be useful for analysing small subsets of data, such as artefacts from compromised computers, or summarising information for an executive report. But from what I've seen, large scale adoption of AI on the defensive side is non-existent."

Gijs Roeffen
CISO at Castor

"The observation that AI has yet to drive groundbreaking offensive techniques is spot on. AI is great at speeding up many tasks, but it's not yet capable of true "game changing" for either side of security. In the long run, AI favours defenders because we have the data advantage. In the short run, attackers may have an edge due to not having to follow any rules while experimenting with AI, and thus learning faster."

Anton Chuvakin
Office of the CISO, Google Cloud

Biggest concerns regarding use of AI in security



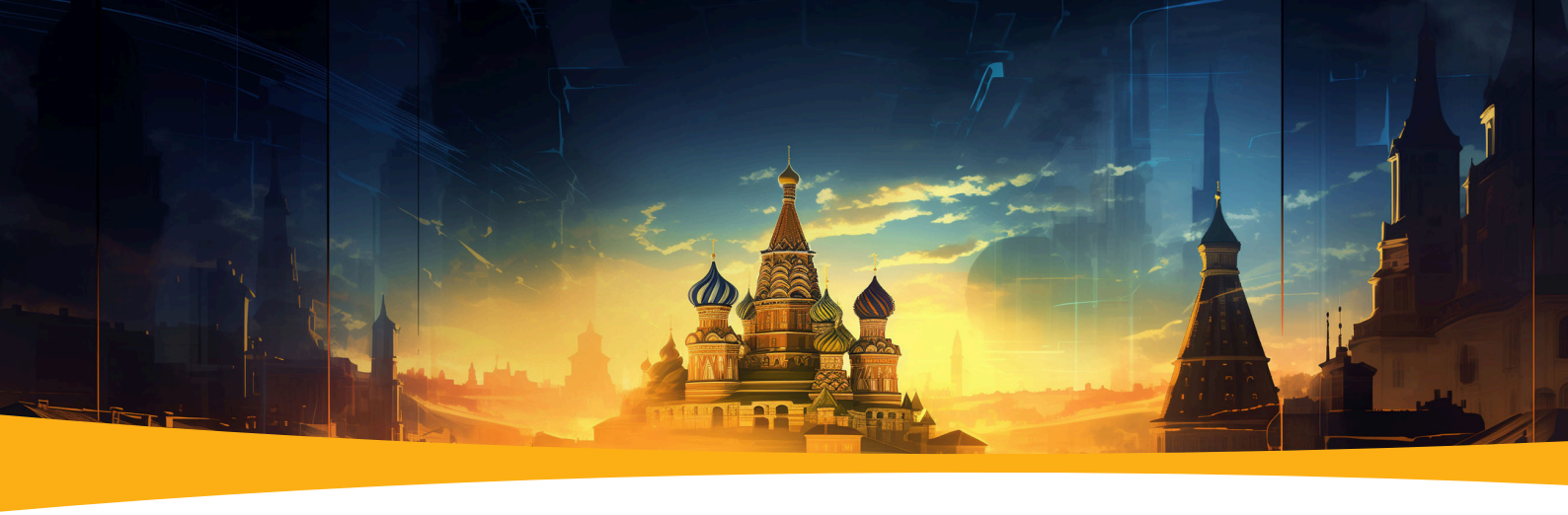
Source: CSA

The Hunt & Hackett perspective

As it stands, AI is being used to greater effect on the offensive rather than the defensive side. Attackers are applying generative AI in areas where it naturally excels - crafting highly convincing phishing emails, social engineering messages, automating reconnaissance, conducting research on targets, and modifying malicious code. These enhancements make their campaigns more scalable, efficient, and difficult to detect.

On the defensive side, however, the approach has been less grounded. Rather than focusing on the (highly specific) tasks where AI can provide immediate, tangible benefits, there's a tendency to apply it directly to the industry's most complex problems without fully understanding them.

Compounding this issue is the rush to position AI as a transformative solution, with many companies leveraging its popularity to attract investment and market attention, often without clear, practical applications. The challenge isn't just vendors pushing AI-driven security tools; it's that the industry is embracing the hype without fully considering the limitations, potential consequences and realistic use cases of AI in cybersecurity. Instead of chasing the next big breakthrough, defenders should focus on using AI on specific (smaller) tasks where it adds clear value - automating repetitive work, enhancing detection of known attack patterns where it supports the human analysts, and gradually scaling to more complex challenges.



CHAPTER THREE

The Influence of Nation States

Key trends

- Nation-states are increasingly collaborating with criminal proxies and contractors, leveraging their capabilities for financial and strategic gains while maintaining plausible deniability and complicating attribution efforts.
- State-directed campaigns were closely linked to areas of geopolitical tension and conflict in 2024.
- China leads the way in terms of pre-positioning and espionage campaigns targeting critical national infrastructure, demonstrating its ability to stealthily compromise sensitive networks and maintain persistence.
- Western nations often treat cyberattacks as isolated incidents rather than recognizing them as coordinated components of modern hybrid warfare strategies.

Lines blur between APTs and cybercriminals

In 2024, the line between nation-state actors and cybercriminal groups continued to blur, as governments increasingly leveraged criminal proxies to advance their geopolitical goals. These proxies allow nation-states to conduct disruptive operations while maintaining plausible deniability, evading direct accountability, and complicating the response from victim countries.

For example, North Korea's Andariel group is suspected of collaborating with the Play ransomware group in a September 2024 attack, highlighting how state-affiliated actors are now leveraging ransomware operations for both financial and strategic purposes.[18] Similarly, Iranian state-backed threat actors have collaborated with ransomware affiliates to target U.S. organisations, gaining initial access and then facilitating ransomware deployment by their criminal partners.[19]

Evidence of collaboration between cybercriminals and state actors is not limited to these cases. Leaked communications from the infamous Conti ransomware group suggest cooperation with Russian government contacts on at least one state-backed cyber operation.[20] Meanwhile in China, the iSoon leak exposed direct links between hacking contractors and state-sponsored APTs such as Double Dragon, Poison Carp and Jackpot Panda. Some groups, like Lazarus and Double Dragon, further blur the lines by conducting both state-sponsored espionage and financially motivated operations in tandem.[21]

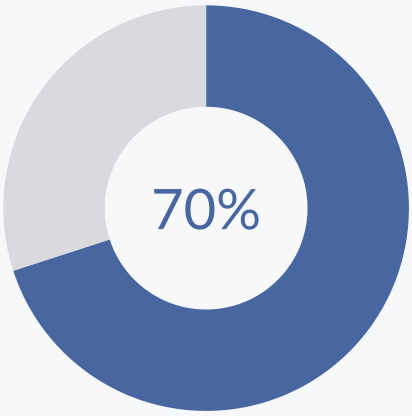
In 2025 and beyond, the overlap between state-sponsored actors and cybercriminal groups is likely to deepen. As geopolitical tensions persist and cyber capabilities advance, nation-states will increasingly exploit the flexibility and deniability that criminal proxies offer.

Nation-state activity focused on conflict zones

In 2024, nation-state cyber operations were heavily focused on conflict zones and disputed territories. The ongoing Russia-Ukraine war has produced a continuous wave of cyberattacks, ranging from disruptive wiper malware campaigns to espionage targeting Ukrainian allies. Over the last year, approximately 75% of Russian targets were in Ukraine or a NATO member state.[22]

"Attacks are coming from a range of sources, whether that's state actors, contractors or standalone criminal groups which can function under an umbrella of protection from the state. Of course, that makes attribution more complex. That's why it's important that government works closely with private sector companies, to get a clear picture of the threats out there, where they're coming from, and how we can defend ourselves."

Ernst Noorman
Ambassador-at-Large for Cyber Affairs



Increase in Russian cyberattacks against Ukraine in 2024, including 4,315 assaults on critical infrastructure.[23]

Unsurprisingly, the Gaza war has sparked a deluge of Iranian cyberattacks against Israel. In the early stages of the conflict, Iranian threat actors quickly repurposed pre-existing access to Israeli targets, conducting opportunistic attacks such as leaking data from an Israeli university. Influence operations were also a prominent feature of their strategy, with online personas like "Tears of War" impersonating Israeli activists to spread anti-government narratives.[24]

Simultaneously, China has continued its targeting of Taiwan, focusing on espionage and long-term destabilisation efforts. Much of this activity can be traced back to the threat actor Flax Typhoon (also known as Ethereal Panda or Storm-0919). Looking ahead, we can expect cyberattacks and influence operations alike to remain an integral part of nations' hybrid warfare strategies and as a means of achieving long-term strategic objectives.

Critical infrastructure under siege

Nation-state actors are increasingly targeting critical national infrastructure, focusing on sectors like telecommunications and energy through stealthy and highly sophisticated campaigns. China stands out as one of the most aggressive players, drawing significant concern from Western states.

A notable example emerged in February 2024, when the US Cybersecurity and Infrastructure Security Agency (CISA) and its international partners issued a joint advisory on Volt Typhoon, a Chinese state-sponsored APT. Volt Typhoon leveraged living-off-the-land (LOTL) techniques to infiltrate US critical infrastructure, pre-positioning itself for potential disruption or sabotage down the line.[25]

"What we saw last year in the US regarding China's pre-positioning is deeply concerning. As coalition countries, we're worried about adversaries embedding themselves in systems that are critical for society - not for immediate use, but with the potential to exploit them in the future. The real challenge is that uncovering one instance doesn't guarantee everything has been detected."

Ernst Noorman
Ambassador-at-Large for Cyber Affairs

Meanwhile, another Chinese state-sponsored actor, Salt Typhoon, was found to have successfully compromised the networks of nine telecom and internet service providers, stealing large amounts of data and accessing the texts and phone calls of high-ranking US politicians. The multi-year espionage campaign targeted officials from both sides of the 2024 US presidential campaign, including the phone of President Trump.

In December, White House officials acknowledged that the attackers were likely still inside the telecom networks, with efforts underway to expel them.[26] These campaigns highlight the scale and sophistication of China's cyber operations against US critical infrastructure - a warning sign for European nations that remain equally vulnerable.

The Hunt & Hackett perspective

When looking at the bigger picture, it's important to recognise that Advanced Persistent Threats (APTs) don't operate in isolation - they function as part of larger clusters of interconnected groups, all advancing a coordinated national strategy. While their objectives and tactics may differ, they are ultimately striving to realise the same overarching goals, as dictated by their governing states.

This coordinated, multi-pronged approach makes these threats much more difficult to counter. To keep pace, defenders need to broaden their perspectives, moving beyond tracking individual threat actors to understanding the larger ecosystems they belong to.

"Our cybersecurity strategy - and the institutions behind it - are still designed to treat cyberattacks as isolated incidents rather than as an integral part of broader hybrid warfare strategies. We need to wake up and change our frame of reference. Otherwise we will be outplayed by the countries that play the long game on multiple chess boards simultaneously."

Jurjen Harskamp
Co-founder and CEO at Hunt & Hackett

CHAPTER FOUR

NIS2 and the Future of Cyber Governance

The NIS2 Directive serves as a key instrument for implementing national cybersecurity strategies across the EU, aimed at protecting Essential, Critical, and Important sectors. Given the evolving threat landscape, the adoption of NIS2 is crucial for shifting from a reactive, incident-based approach to a more strategic defence framework - one that enables a stronger response to the hybrid warfare threats we now face.

Key trends

- Cybersecurity is set to become a boardroom issue in 2025, as accountability falls to business leaders.
- The Directive introduces stricter requirements for incident reporting, with the aim of fostering greater transparency and collaboration across the cybersecurity community. However, legal, contractual, and financial risks create potential barriers to information disclosure.
- Supply chain requirements may drive organisations toward larger, more well-established suppliers. While this improves risk management, it may also stifle innovation.
- A core challenge of NIS2 is ensuring it leads to real security improvements rather than becoming a regulatory checkbox exercise. Organisations must move beyond compliance and focus on assessing key risks, understanding threats, and building resilience in a way that is both practical and effective.
- The effectiveness of NIS2 will likely depend on its execution. If absorbed too heavily into the legal and compliance domain, it risks losing its intended impact.

Cybersecurity will become a boardroom issue

The NIS2 Directive is transforming how organisations address cybersecurity, elevating it from a technical concern to a core governance priority. By explicitly requiring business leaders to take responsibility for compliance, NIS2 ensures cybersecurity is no longer something left solely to IT/OT departments.

"NIS2 should be helpful in terms of creating a lot more awareness within the organisation. Previously cybersecurity was seen as something for the nerds to deal with, but now that responsibility is shifting more to Board level- and that's where it needs to be."

Kelvin Rorive
CISO at ICT Group

"What's really important is that it moves responsibility to the boardroom. You cannot say, well, I didn't know about it as a CEO. That's something for my technical department. No, it's a C-suite level discussion now. And that I think is really crucial," says Ernst Noorman, Ambassador-at-Large for Cyber Affairs.

This paradigm shift is also driving organisations to integrate cybersecurity into their long-term strategies.

"We want to get to that point where cybersecurity is something that you take into consideration in your annual planning - embedded in the core business strategy of every organisation and accompanied by a thorough analysis of risk appetite."

Moshgan Wahedi
NIS2 Program Manager at NCSC-NL

Companies face increased reporting obligations

The NIS2 Directive introduces stricter incident reporting requirements, mandating organisations to provide information about cybersecurity incidents within specific time frames. While this aims to foster greater transparency and information sharing, the practicalities of implementation are still unclear.

"When does an incident become reportable?" asks Kelvin Rorive, CISO at ICT Group, noting the ambiguity organisations face in determining thresholds for reporting. With multiple incidents occurring daily, distinguishing between minor events and those warranting regulatory attention poses a potential challenge.

Policymakers alone cannot effectively define these thresholds, says Moshgan Wahedi, NIS2 Program Manager, NCSC.

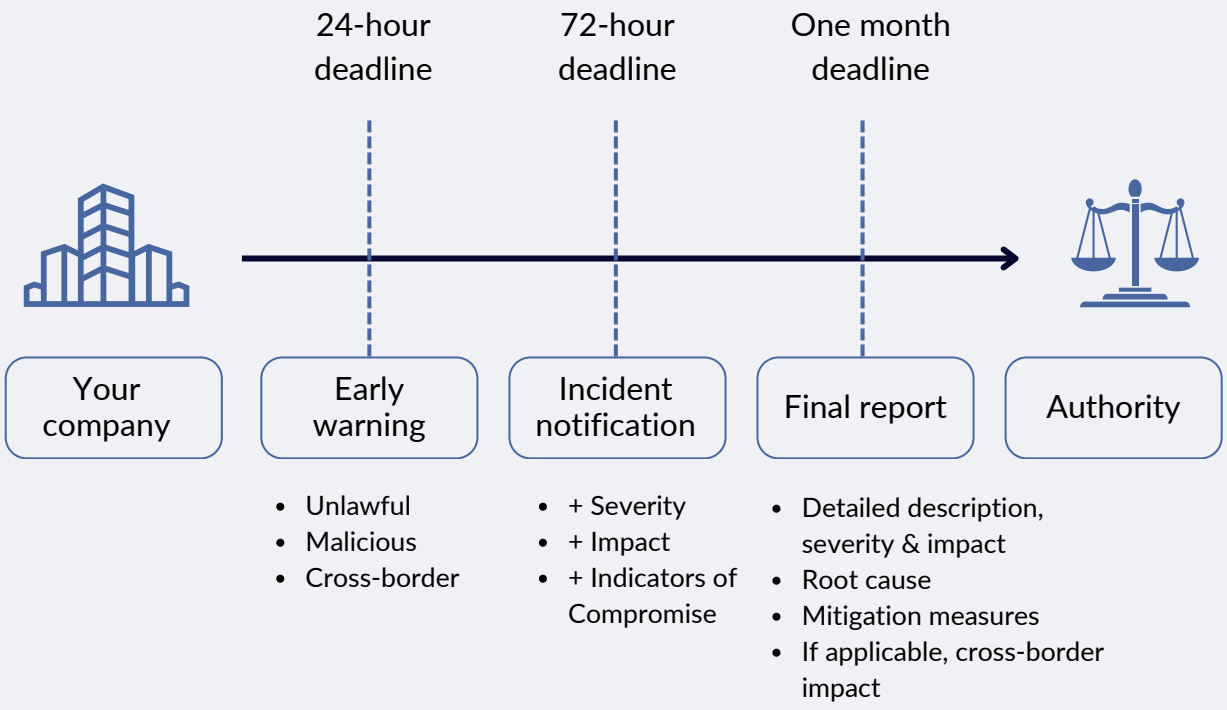
"We shouldn't wait for policymakers to decide what constitutes a reportable incident. CISOs, SOC analysts, and CTI specialists are the ones who understand their environments best. We need to empower them to share information - not just with us but with the entire cybersecurity community."

Moshgan Wahedi
NIS2 Program Manager at NCSC

"It's so important for organisations to be more open about attacks," adds Ernst Noorman, Ambassador-at-Large for Cyber Affairs. "Some organisations feel ashamed of being attacked, but they shouldn't - everyone is being attacked. It's better to be open, so we all can learn from it. It's a shared responsibility to keep society safe."

Efforts are underway to simplify incident reporting and vulnerability disclosure, with a focus on developing easily accessible tools to streamline the process. "We [at the NCSC] must also ensure we're approachable," notes Wahedi.

NIS2 incident reporting timelines



Barriers to information sharing

While increased information sharing is widely recognised as key to strengthening collective cybersecurity resilience, several barriers hinder organisations from disclosing information freely. Legal and contractual constraints often have a chilling effect - broad confidentiality clauses in NDAs create uncertainty about what information companies can share and with whom. Additionally, technology vendors may impose restrictions on disclosing vulnerabilities in their products, further limiting open communication.[27]

Financial concerns also play a role; organisations may fear that participating in information-sharing initiatives could be seen by insurers as an admission of vulnerabilities, potentially resulting in higher premiums. [28]

While NIS2 marks a significant step forward, addressing these underlying challenges is crucial to achieving meaningful and sustained improvements in cybersecurity resilience.

"Businesses understand that sharing certain information can expose them to liability and reputational damage — risks they'd rather avoid. There's still a lack of awareness about the real challenges organisations face when it comes to transparency."

Jurjen Harskamp
Co-founder and CEO at Hunt & Hackett

Oversight of digital supply chains

NIS2 introduces stricter oversight of digital supply chains, a shift that is both necessary and complex. Companies will need to evaluate their suppliers' cybersecurity maturity more rigorously, which will likely have a significant influence on the vendor selection process. While this emphasis on supply chain security has been (broadly) welcomed, its implementation poses potential challenges for both customers and suppliers.

Currently, suppliers are inundated with varying security questionnaires from potential customers, creating a heavy administrative burden. "We need to find a more structured, commonly agreed way to inform each other about our security maturity as suppliers," notes Kelvin Rorive, CISO at ICT Group.

However, the push for compliance and maturity signalling could have unintended consequences. Stricter regulations and legal liabilities may lead organisations to become more risk-averse, favouring larger, more well-established vendors over smaller players that lack the resources to meet the necessary security requirements.

"It is no secret that innovation in the security space comes from the younger start- and scaleups, and not so much from the large established providers. So, it's easy to see how this could stifle innovation," says Jurjen Harskamp, co-founder and CEO at Hunt & Hackett.

"Smaller companies with promising technology may find themselves shut out of the market. This comes at a time when we are increasingly aware of our reliance on U.S. security technology and the lack of viable EU alternatives. While the initiative has good intentions, it may inadvertently create additional barriers to achieving this strategic goal."

Jurjen Harskamp
Co-founder and CEO at Hunt & Hackett

Additionally, this shift must be balanced with the risk of superficial certifications. As Gijs Roeffen, CISO at Castor, observes, the market has already seen companies achieve certifications like ISO or SOC 2 through templated processes that fail to reflect genuine maturity.

"We've encountered suppliers with SOC 2 certifications that were only months old, and upon closer inspection, we found their security measures were ineffective and generic. I fear this could become the case with NIS2 as well."

For smaller suppliers, achieving compliance may feel overwhelming, but simplicity and focus on basic hygiene remain key. "What we lack as a society is simple enforcement of the basics - don't worry too much about adding all the bells and whistles," adds Roeffen.

"The small manageable measures will go the furthest in laying the groundwork for your cyber security posture. Obviously, if you're a high-risk organisation - a nuclear facility for example - then it's an entirely different ballgame. But for most companies out there, doing the basics is still the best way to go and will have the highest chance of keeping you out of the dark."

Gijs Roeffen
CISO at Castor

Not just a box-ticking exercise

As the Netherlands prepares for the implementation of NIS2 into national legislation in Q3 this year, many organisations are working to understand the Directive's requirements and implications. Unlike a rigid, prescriptive checklist, NIS2 adopts a broader, holistic framework aimed at strengthening cybersecurity resilience across sectors. While this approach encourages flexibility and adaptability, it can also be challenging for companies to navigate, as the absence of clear-cut guidelines leaves room for varied interpretations.

"It's extremely confusing to figure out the right way forward," explains Gijs Roeffen, CISO at Castor. "Everyone has their own opinion on what we should be doing, what the right or wrong approaches are, and that's a missed opportunity in my opinion."

This underscores the importance of moving beyond mere compliance to focus on risk-based decision-making. “If I am compliant, I am not necessarily safe,” warns Kelvin Rorive, CISO at ICT Group. “But if I can prove that I’m secure, then I should be compliant.”

Achieving this balance requires organisations to start with the basics: identifying key assets, understanding the threats they face, and assessing their current resilience. “In order to be compliant, you first need a proper analysis of your interests and risk appetite,” advises Wahedi.

“I would love to see organisations looking at NIS2 from a more multidisciplinary perspective, ensuring that not only the compliance people, but also the technical people, and the people who are actually driving the core value of their business are able to sit together in one room - they'll be able to look at it from a very different perspective.”

Moshgan Wahedi
NIS2 Program Manager at NCSC

The Hunt & Hackett perspective

NIS2 presents a significant opportunity to strengthen national cybersecurity strategies across the EU, providing a framework to protect Essential, Critical, and Important sectors. Its adoption is crucial for shifting from a reactive, incident-based approach to a more strategic defence framework - one that improves resilience against hybrid warfare threats. However, key challenges remain. While NIS2 aspires to bring technical, business, and compliance teams together, in practice, it risks being absorbed into the legal and compliance domain. Rather than fostering a multidisciplinary approach, organisations may find that compliance and legal teams dominate the conversation - sometimes at the expense of real security improvements. The success of NIS2 will ultimately depend on how well it is executed.

A key emphasis of NIS2 is on reporting and information sharing - an initiative that, in theory, should strengthen collective cyber resilience. However, the reality is more complicated. Many organisations face legal, contractual, and reputational risks when disclosing incidents, making full transparency easier said than done.

Meanwhile, supply chain requirements present a different challenge: market consolidation. Larger, well-established vendors will find it easier to navigate compliance, while smaller companies will likely be priced out of competing. This dynamic risks stifling innovation, as companies increasingly default to 'safe' choices, favouring vendors with recognised credentials like ISO and SOC2 certifications, even when they aren't strictly necessary.

The market has yet to find an efficient way to balance risk management with accessibility. This comes at a time where we are beginning to realise the impact of Europe's reliance on US-based security technologies. Addressing such strategic challenges requires difficult decisions about prioritisation, ensuring that well-intended regulations do not inadvertently create new barriers.

At its core, NIS2 represents a crucial step towards a more secure digital ecosystem. But the ultimate question remains: how do we ensure that these regulations lead to better security outcomes - rather than just more comprehensive paperwork? This challenge is as old as the cybersecurity space itself. If it's not addressed, NIS2 risks becoming ineffective from the outset. This should not be allowed to happen - effective national cybersecurity strategies are essential, especially as cyber operations continue to play a central role in hybrid warfare, used as a key instrument for achieving geopolitical and financial objectives.

References

1. Internet Crime Report. (2023). In *www.ic3.gov*. Federal Bureau of Investigation. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf
2. Poireault, K. . (2025, February 19). *Akira and RansomHub surge as ransomware claims reach All-Time high*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/akira-ransomhub-ransomware-claims/
3. *Law enforcement disrupt world's biggest ransomware operation* | Europol. (n.d.). Europol. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
4. The Hacker News. (n.d.). *Exit Scam: BlackCat ransomware Group vanishes after $22 million payout*. https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html
5. The Hacker News. (n.d.). *Exit Scam: BlackCat ransomware Group vanishes after $22 million payout*. https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html
6. Kovacs, E. (2024, June 6). *FBI Says It Has 7,000 LockBit Ransomware Decryption Keys*. Security Week. https://www.securityweek.com/fbi-says-it-has-7000-lockbit-ransomware-decryption-keys/
7. *Threat Report*. (2024). Eset. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf
8. Internet Crime Report. (2023). In *www.ic3.gov*. Federal Bureau of Investigation. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf
9. Hines, A. (2024, July 23). *Adversary-in-the-Middle Cyber attacks: The growing threat to business emails.* Dean Dorton - CPAs and Advisors. https://deandorton.com/adversary-in-the-middle-cyber-attacks-the-growing-threat-to-business-emails/
10. Weinert, A. (2024, November 13). *Defeating Adversary-in-the-Middle phishing attacks*. techcommunity.microsoft.com. https://techcommunity.microsoft.com/blog/microsoft-entra-blog/defeating-adversary-in-the-middle-phishing-attacks/1751777
11. Bleih, A. (2024, October 1). *A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more*. Cyberint. https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/
12. Rapid. (2024, August 1). *Rapid7 releases the 2024 Attack Intelligence Report*. Rapid7. https://www.rapid7.com/blog/post/2024/05/21/rapid7-releases-the-2024-attack-intelligence-report/
13. Rapid. (2024, August 1). *Rapid7 releases the 2024 Attack Intelligence Report*. Rapid7. https://www.rapid7.com/blog/post/2024/05/21/rapid7-releases-the-2024-attack-intelligence-report/
14. *What is Ransomware as a Service (RaaS)? | CrowdStrike*. (n.d.). https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
15. *How much is the phish? Underground market of phishing kits is booming*. (2020, April 15). www.group-ib.com. https://www.group-ib.com/media-center/press-releases/how-much-is-the-phish/
16. Makrushin, D. (2021, March 19). *The cost of launching a DDoS attack*. Securelist. https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
17. Bleih, A. (2024b, October 1). *A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more*. Cyberint. https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/

References

18. Montalbano, E. (2024, October 31). *North Korea's Andariel pivots to "Play" ransomware games.* Dark Reading. https://www.darkreading.com/endpoint-security/north-korea-andariel-play-ransomware
19. Iran-based cyber actors enabling ransomware attacks on US organizations | CISA. (2024, August 28). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
20. Burgess, M. (2022, March 18). *Conti leaks reveal the ransomware group's links to Russia.* WIRED. https://www.wired.com/story/conti-ransomware-russia/
21. Lumley, R. (2024, March 11). *iSoon leak sheds light on China's use of extensive hacker-for-hire ecosystem.* Hunt & Hackett. https://www.huntandhackett.com/blog/isoon-leak-sheds-light
22. Burt, T. (2025, February 18). *Escalating cyber threats demand stronger global defense and cooperation.* Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/
23. Mukhina, O. (2025, January 12). *Russian cyberattacks on Ukraine surge 70% in 2024 with 4,315 assaults on critical infrastructure - Euromaidan Press*. Euromaidan Press. https://euromaidanpress.com/2025/01/12/russian-cyberattacks-on-ukraine-surge-70-in-2024-with-4315-assaults-on-critical-infrastructure/
24. Burt, T. (2025, February 18). *Escalating cyber threats demand stronger global defense and cooperation.* Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/
25. *PRC State-Sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | CISA.* (2024, February 7). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
26. Kapko, M. (2024, December 4). *Feds raise alarm on China-linked infiltration of telecom networks.* Cybersecurity Dive. https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576/
27. Koepke, P. (2017). *Cybersecurity Information Sharing Incentives and Barriers*. In mit.edu. MIT Management Sloan School. http://web.mit.edu/smadnick/www/wp/2017-13.pdf
28. *Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection.* (2020). 12th International Conference on Cyber Conflict. https://ccdcoe.org/uploads/2020/05/CyCon_2020_4_Nweke_Wolthusen.pdf

HUNT & HACKETT

Hunt & Hackett was founded in 2020 by Ronald Prins (co-founder Fox-IT) and Jurjen Harskamp (former executive Fox-IT). Hunt & Hackett is a privately-owned Dutch company based in The Hague, the Netherlands, and governed by stringent national and European standards on privacy and security. A fast-growing team of highly experienced security specialists and upcoming talents is protecting customers against their sector- and organisation-specific threat landscape, including the most sophisticated APTs.

Want to know more?

Join one of our CyberConnect roundtables

Questions or want to get in touch?

+31 70 22 0000

info@huntandhackett.com

www.huntandhackett.com